Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

«Криптографія»

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студенти групи ФБ-93
Приходько Андрій
Шахова Катерина

Київ – 2021

Мета роботи : засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера

Хід роботи :

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

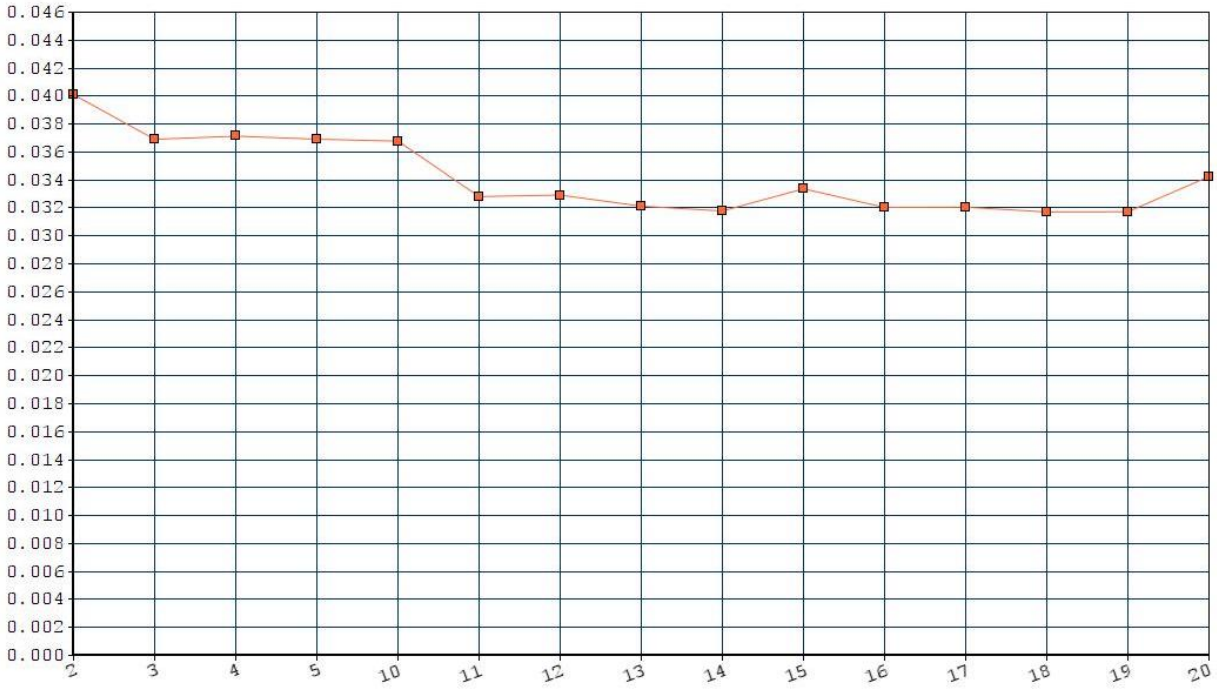
Завдання 1-2

Для шифрування обрали текст чудової пісні гурту «Порнофільми» - «Я так соскучился». Порахували індекс відповідності відкритого тексту - 0.051935851263582355. Були підібрані ключі для шифрування довжиною 2-5,10-20 знаків. Для кожного варіанту пораховано індекс відповідності. Результати у таблиці нижче:

Довжина ключа	Ключ	Індекс відповідності
2	иа	0.04009850093883707
3	щъе	0.036908301782251365
4	фяыз	0.03713362267984117
5	рфдхд	0.036919383137870534
10	роургикпум	0.03677778803829224
11	эчтшнетквзс	0.03281189398836458
12	нбюъжчгдбтпр	0.03292147628282082
13	бкэщфыиовъпъс	0.03212731246344692
14	ейеъсолпйяьэрж	0.03178255917751716
15	швцюкбтшящшсотх	0.03336842429279404

16	йьглыччкзрбзцквс	0.032039892880229015
17	мдщсжпубдиокитююю	0.03205589928279004
18	дюсушсюбугпчкеацдй	0.03171237725859575
19	цырэопьъыядищлрфдхц	0.031725921137685846
20	чпчыцсеилщфйэкчъртум	0.03424385138670853

Діаграма значення індексів відповідності для вказаних значень r :

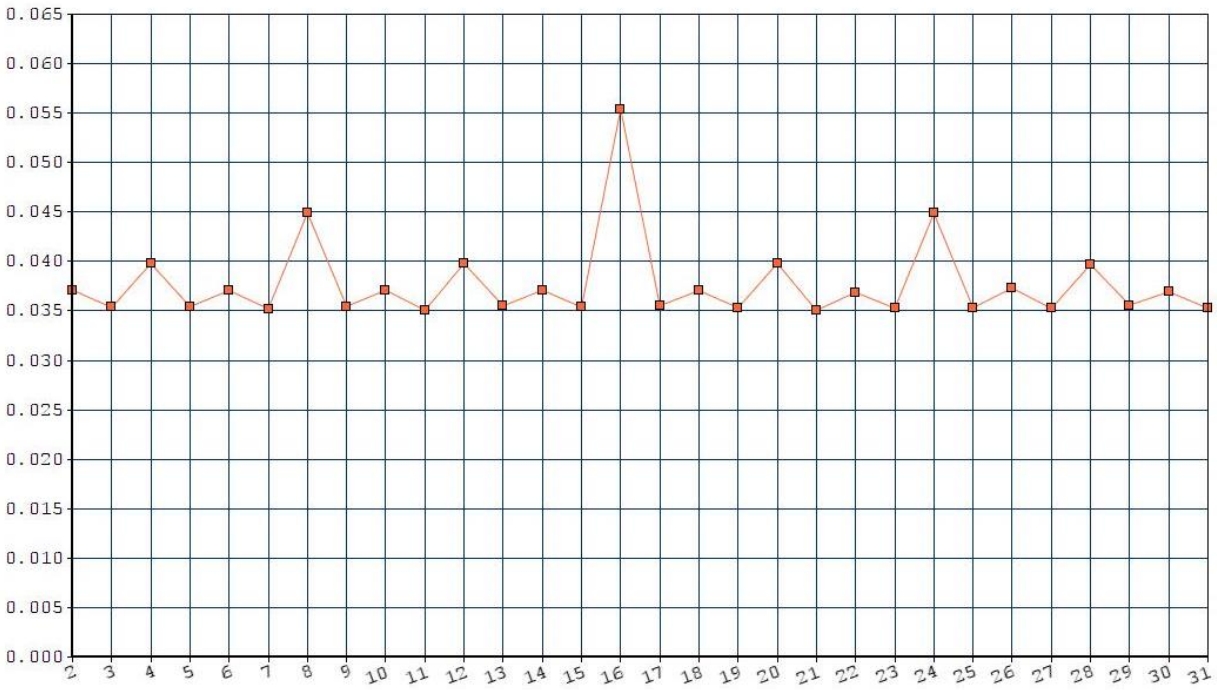


Завдання 3

Для цього завдання ми розділили текст на довжини різних блоків та рахували індекси відповідностей для кожного з них, щоб знайти можливу довжину ключа. Таблиця результатів наведена нижче :

Довжина ключа	Індекс відповідності	Довжина ключа	Індекс відповідності
2	0.037096826206553676	17	0.035524349460576386
3	0.03535245194471151	18	0.037051140206933175
4	0.03979351166739004	19	0.03531599104429486
5	0.0354351293936251	20	0.03979839848540342
6	0.037052368586566846	21	0.035056696947883076
7	0.03522360497899179	22	0.03688094981192191
8	0.04491213203766699	23	0.03526676001305198
9	0.035450251570776165	24	0.04486292731353409
10	0.03709763005817015	25	0.03531687664602463
11	0.035062146465428885	26	0.03731086887465935
12	0.039788848438709196	27	0.035247591055245484
13	0.03550919719241092	28	0.03969086727168179
14	0.037093872461702884	29	0.0355849038850587
15	0.035384371390931875	30	0.036928328869868694
16	**0.05539766505382551**	31	0.03527346532158509

Діаграма значень індексу відповідності одержаних при встановленні довжини ключа шифру Віженера :



Отже, з’ясували, що ключ має довжину 16. Далі розглядали кожен із 16 блоків окремо. Ці блоки по суті зашифровані шифром Цезаря. І за допомогою частотного аналізу ми можемо знайти ключ для кожного блоку та отримати ключ для всього тексту в цілому. Взявши найчастішу літеру «о» ми отримали ключ «деколисоборойоей». Розшифрований текст мав певні неточності , але за допомогою логіки та змістовності тексту ми змогли вручну поправити ключ та отримати повністю розшифрований текст. Так ми отримали ключ «делолисоборотней».

Шифрований текст :

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбъъюбяцбаъъшрсеццшиуусы
юуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхсаацспнрцроцщйьэьгимхдрзяэксыжяфуэнрчхбвуццу
улббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоьврвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзцц
эьцдыыгышътъниикэнчцввьуэыаскыгсэуатгьообуэмкыщшэбшгаьуъьбшыждытлнцнюътамщрсцуддьщюощажъгэ
адчсскщтщущъъъяючьдыхчнцрфюооуюпммчцяъъющщгьсоецюькщмнняэшцебувястюоскчоццьмеущшаяущясъь
хиыцнающъебкчйпотхсуушршъщфщмьуылфголцэугяефтншаршцяойыыъдччзрлршццыйятудымйфтжунгвьуйфб
знзопнхцашцщйсшчъпкасафэщрвштъляэнлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцььгъъюеуныйрзыж
нтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцдйшцчряпъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыц
ытхшьрщяяуьпачшбцткутщйбьеувуэйтчйлуазнвапщмугякъцзрышщцтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьу
ючвеыднэкаыгбойэогтросамйцруьтыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлелк
йудьымцтоссуфырцбтфябшацпьпбэбыгсяльаучпччркоьтхсежышцыччфуряэцькзуфофъуъикцоццвкпплеяислйзы
ьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжчътдщмлпщъяатбвядпноуупщухюькрюяб
хчйстщяэртюпярудюдрикьknльоиофошттожтуълъцщэыюъеъекпгпоэньмшуыьфтпъиуыьорээжюбаятсцдфлщзюц
ьеувйыпфщйпыоьхмчщуышапатхштъыцикжъеоэнчхтлрашиаюйъхюфьхсхшэяэкщцзуэзъъашфуухшнвайпаояъуо
хрщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичхфщшщсюьеьбатябслхюшлкстпююсацхйхэуажсащба
юшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмйреэуыньруоъьюуъцукыурхбщцшхюттсцбрсщтсшрюрръшуьк
кшуцдшнсочрчдччршпющнюувьтютфшхмчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпр
эйчыжфдцэцъыгкиоъощнтцдцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыечшулйпш
опцхоукхъеьхчкнэксршыэаршьнпчсъщеръыьоузыатцфмушэыргьныхрвтйсцухююосмъцьэакччршмоохцьшуэкэл
жспхлчщхжбубэьфхпйофыонрььпшрхнпефхдттрщнщйжмэаюрьккмыщсюоеьсыаючсжуэшлтвудьфысъкъруэюкх
сэсьвцфъатсенунипзйчеоясхьиустуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрййхуъбэщгрпрррктичерух
хцэбйбфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаьпрььсобяэтйчжешцрцзумьщячянайчжюрпсржтхыъ
мкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйккьуоылгфэерчйлщщфаьтуышчгнэфачошрьцрюрятсзофтющь
зуомуъятъйщмгнтщэюьгщхыяиочцпыйнащъйяпэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмшъ
щнюдхвунхръйцыофчехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцукхзчхйчщупйщ
ъяэйбьььахоснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэрлцаюйьсючякцмншьнцъыжттцшх
счхчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтйизьучржосехрямссмрлрхиэцсочбцнрчзуъььньшбово
юыьосбьшщшяррюшытсрокедцауссбжгхтпкнйтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьч
цдйоыкяикрдпюажлхулббщерехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуаруныьуяюъоу
щяфыоьихэсуфщтрефууьуэргумньыапуоххртъъуьсобяэнжсцбэуцщьшщбаъябнчэюэщщьууюгтапаюешпырсаьту
вцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжцрпктюниуьютфшндрщс
щцюхбгюачшсцтищцьшсхфырыспцоекнэщфязэыхяьыреоупмсржъпщютиызшфеьоппспьщюсэнзцтсубъъбунцыя
счтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугышуюатоухуылмьузотжътьоржщцзацьцрречъурдзртрхщ
чууърнекшфнмйэцыабшбэвнзоирурщчящбсрщэнийьумюлбсаэяпшфкокмтлъпурюжжхыъмзчлтушлжкццюрхяыи
фдцучмгьюутгтэеуцкыущйщабахщчцъьцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайу
шшхцтэцмъсцэньукяюрэнййцбьщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйфешурчятдьвьфхръгпьа
жяыонцюадыичтплхлувнтцыкяткчоушелъцщэыююютюфчгцлргрвкпыбысшцчхчрыжмубтатьэйтчйхюфзнхуеошэв
хрзитщэызэьрьбючсншйхрбцтсьуэшщъшцыжуцйъцвщжехсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпосна
юпхтцлтфчпшвццтюжхрстщкъцтжусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыф
дьтжъбкцапъыохнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшскцмошутшряло
чоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьтяыжеэйюхцйруньцдюьрюшяфыкцсафэыивоеьыычокъсафъл
ххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэклдрщпиъяъгяъьвттохпщщзтяежщюрччфч
цкынцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевтмхйхшьоцдэпаауушкцмдщэуыэооо
ьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытйфупыщляхеьаьфйдлхкьащшяыоушхеднфтфыцв
рюбиосьэтзйснкрлхсцгяъьвтукфктооивонаюсаъклййлнъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкн

рнббъъсюбышнюхжйзеуртзгьдьшъфьухтюзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййпплшиъяась
чьфыюоонфцьуцслохзчьунйчьшухсцгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрчсшвйищцъгггщйрюсащеъцкыо
ьгвшоьуьцтрйфеьэщуяфжышуфюкюленупнюцксфуьахспнщэуыэпьщюьбэкнйррыщщюойрюхюылцтоэьвхяяукоа
тчлоеаццьцвабрыуяифчихщпшгцярцбшъпцощфщтпиюыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзуп
щкпхьсьтксьущтплбъшсрмуэцчптоьтрчщэбоойбьгшультьррумзугяюяднзспувщрхяявьаынцфчфчыуэяцщпрхштчу
ытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмыщцднпайрщрртяыбюгжъякфажжщупяпмцзуяскъгчзялфмгт
эюяаотдщзичмрюьгэхючыйожэуязкфюбффояюпчйфцоэдцхбааьчюшытпшуъшцяуоэыаруъпшсумхясппфуяхдьхч
лыщкщщйсфуаохолеоомгуожаяьгпусрфыьэрубрюрряиснйрлъухмышутуйтхчрфыцьъцежышцщъеамчрщзхмгтцы
ббэелпкшцкцхбсърыъпецмкщюпывялцеэасййстжгщчщбньыючекцтжжщщчбутузкбышъпунщрхюьнббцхъефчзич
мрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньызчрьсошцэхбтхюшхзйвчтоъшсрйщгцчрукпнсыутярлоъяднрч
ммнуъъюьгузувъноыеьйъцвщжьсгасеъжуугнустжышчъпмсрешцкнчуеыхряыоцйфыоннхыпчфояхрйзегящщуьйъ
шпэхлцмплъутяюпарщфъкътумюлпюьнрхячшнсжълювнуыжшгыъюацтззнмифуъуаощпммпдшбцхсебялцвнмндз
ущщтдюпштпвытртзщчънаумкэцитфчфещыцнфшпэютямръгцчуъъсцноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъ
ютьцтсрелхцпьщюытьхсжавыщфэутахюасултохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцвьыюрзсуфхцц
дъоьуьбыйндтшьоцыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхюйкгрыунрд
оцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщтющшншонувыаьхчжкыццщы
юьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьцанрлецйэыходтхячсзйхржжшгэжпююгащцогрьн
ьтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфекяьвн

Розшифрований текст :

понятноеделокультурунасильновчеловеканеворknешьвордусиэтудовольногрустнуюистинузналинавер
ноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальстванесделало
сьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцеремон
ийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюд
скаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещенемал
олюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисв
етозарныевысотыдухавеликихрелигийивечныйпоискcмыслажизниземнойпитающийистинноеискусств
ониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыега
тинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестественноедлябольш
инстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамииневобычномпо
ниманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениик
отороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиеритуал
овивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаженевнимательном
унаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатмож
етнапримервприсутствииженщиныпроизнестибранноесловоиливысморкатьсяприлюднопрямовземлю
послечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекповзрослелиза
матерелвтакомсостоянииидушиизменитьегокакправилоуженельзяразвечтомудроенебовразумиттакили
иначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневместноа
увещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетко
нечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказыв
алсяздесьлишьпослужебнойнадобностиводкаксегоднянесмотрянапротивныйнавевающийхандрудожд
икбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблизкомуиудачномузавершениюо
чередногоделакконцуподходилорасследованиеоцелойсетичетырезаведенияединовременноподпольны
хопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександриювдохновл
енныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнямиилавкам
ииесликприбылямотторговлиспиртныминапиткамиудастсядобавитьещеидоходыотопиумокурениятом
ожнобудетподуматьорасширениипредпринимательстваоприобретенииновойнедвижимостиииншаллаб
ытьможетдажеобустановленииконтролянадвсемихарчевнямиилавкамиразудалогопоселкаатамоченьск
оровпринадлежащихлагашузаведенияхнемногочисленныеноверныеегослужителиоборудовалиспециа
льныезакутыгдекуслугамжителейигостейхутуновывыстроилисьудобныележанкиикурительныеприборы
прасадпредлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейпосе
тителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняземразудал
огоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпрасадзабылоглавномиустрем
илсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниемунепринадлежавшиечембольшеохвачено
заведенийтемвышеприбытоктаксправедливополагаллагашобращатьсяквэйбинамдлярешенияВозникаю
щихразногласийбылоневхарактереобитателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользо
валсяпопыткиздешнихжителейсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаранееп
одготовилсякстычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсостеныдвуствольно

еружьедедаиприлюднопрямопосредипереулкаотпилилстволыпослечегосталходитьпохутунамсобрезо
мзапазухойидажепрозвищеполучилобрезагаместныежителирастерялисьопиумокурильнирасцвеливпо
селкенесообразнопышнымцветомлагашподсчитывалбарышиновеликийучительвдвадцатьвторойглаве
беседисужденийнезрясказалянезнаюниодногоправлениякотороебылобыбесконечнымисамовольнопри
своенныйпрасадомнебесныймандатместногозначенияужеуплылизегорукхотялагашещеинеподозревал
обэтомвскоренесколькочеловекпотерялитрудоспособностьинтерескжизниисамоездоровьевследствиеч
резмерногоупотребленияопиуманасонгрядущийавандевятыйпопалвбольницуулусноеведомствонарод
ногоздоровьявсестороннеизучилопричинузаболеванияванаивскореобрезагасамтогоневедаяпопалвпол
езренияуправлениявнешнейохранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяк
овачжанабагссимпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепен
нопревращаетсявсведущегоипытливогомастерасыскногоделарасположениевсехзаведенийгдекурилио
пиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподробныеспискивсехподданн
ыхимевшихотношениекраспространениюопасногодляздоровьяпорокауправлениевнешнейохранысосл
овочевидцевсоставилочленосборныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзапра
вилойитакчеловеконарушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвграждан
скоеплатьезатроесутокнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротив
управнымделаминынчевечеромпристечениизначительныхсилуправленияодурманиваниеордусскихпо
дданныхопиумомрешенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезавед
енияабагсяковомчжаномзадерживаютзаправилуиегоближниковкаксталоизвестновечерниечасыпослео
бходасвоихвладенийивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикороталвнесо
образномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепель
ницепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонаприв
ычномместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданногоко
зюлькинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастергань
цзянмошуобещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхал
атомбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгу
стеющиесумеркибесконечныйдождьпора

Висновок : виконуючи дану роботу ми змогли проаналізувати шифр Віженера. У ході роботи вивчили поняття індексу відповідності та за його допомогою змогли «взламати» текст, що був зашифрований шифром Віженера